Managing Internet and Intranet Information for Long-term Access and Accountability

Implementation Guide

A Paper Prepared by the IM Forum
Internet and Intranet Working Group

September 24, 1999

Foreword

The following *Implementation Guide* should be read in conjunction with *An Approach to Managing Internet and Intranet Information for Long-term Access and Accountability*. Together, the two documents respond to the need for government-wide direction on managing records and publications within departmental networked facilities, including the Internet, intranets and extranets. The Information Management (IM) Forum Internet and Intranet Working Group prepared both documents on behalf of the IM Forum.

The documents amplify the *Government of Canada Internet Guide*, which can be found at <http://canada.gc.ca/programs/guide/main_e.html>.

The *Approach* and *Implementation Guide* represent almost a year of work by the Working Group, which first met in April 1998. The initial objective of the Group was to provide "an articulated common approach to record keeping on the Web." In determining how best to do so, the Working Group looked at several critical questions, not the least of which is, "When is information on a Website published information and when is it a government record?" In addressing this issue, the Working Group has focussed on two requirements: capturing records as evidence of business activity and managing long-term access to published information. By approaching the issue this way, we feel we can jointly mobilize the strengths of both the library science and records management disciplines, on behalf of our clients.

The documents will likely evolve over time as our understanding of the relevant management issues take shape. In the meantime, both the *Approach* and the *Implementation Guide* provide a broad framework for developing institution-specific solutions and helping the government as a whole effectively manage networked information both for long-term access and accountability.

We encourage written comments about this document. Please send them to the Chair of the IM Forum.

Rosemary Murray-Lachapelle
A/Director
Office of Government Records
National Archives of Canada
395 Wellington Street
Ottawa, Ontario
K1A ON3

Telephone: (613) 947-1513
Facsimile: (613) 947-1500
Internet: rmurray-lachapel@archives.ca

You can obtain a copy of *An Approach to Managing Internet and Intranet Information for Long-term Access and Accountability* from the following address:

The Office of Government Records
National Archives of Canada
395 Wellington Street
Ottawa, Ontario
K1A ON3

Telephone: (613) 947-1515
Facsimile: (613) 947-1500

Acknowledgements

The IM Forum Internet and Intranet Working Group prepared this *Implementation Guide* and the *Approach to Managing Internet and Intranet Information for Long-term Access and Accountability*. Contributing members of the Working Group include the following people:

Suzanne Beaudoin, Public Works and Government Services Canada—Canada Site
Nancy Brodie, National Library of Canada
Tina Cacciato, Human Resources Development Canada
Fernand Comeau, Health Canada
Diane Crouse, Foreign Affairs and International Trade Canada
Sharron Curley, Public Works and Government Services Canada
Judy David, Public Works and Government Services Canada—Publiservice
Jerry Donoghue, National Archives of Canada
Greg Eamon, National Archives of Canada
Nora Fontaine, Foreign Affairs and International Trade Canada
John Fysh, Department of National Defence
Julia Goodman, Agriculture and Agri-Food Canada
Sue Hanley, Indian and Northern Affairs Canada
Lark Hodgins, National Capital Commission
Dan Lemieux, Office of the Solicitor General
Jim Lowe, Industry Canada
Doug McDonald, Health Canada
Paul McLaughlin, Department of National Defence
Andrew Morgan, National Archives of Canada
Rosemary Murray-Lachapelle (Chair), National Archives of Canada
Marilyn Sullivan, Indian and Northern Affairs Canada
Craig Taylor, Department of Canadian Heritage
Melissa Teasdale, Public Works and Government Services Canada
Donna Warren, Department of Canadian Heritage

Special thanks are also extended to the following people for their contribution:

Helen Apouchtine, Human Resources Development Canada
Diana Dale, Department of Canadian Heritage
Cecil Somerton, Canadian Coast Guard
Ginette Fauvelle, National Archives of Canada

Managing Internet and Intranet Information for Long-term Access and Accountability
Implementation Guide

Table of Contents

1. Executive Summary 1

2. Management Framework 4
   - 2.1 Introduction 4
     - 2.1.1 Purpose 4
     - 2.1.2 Background 4
     - 2.1.3 Scope 4
   - 2.2 Information Management Principles 4
     - 2.2.1 Supporting Decision Making 5
     - 2.2.2 Managing Evidence 5
     - 2.2.3 Managing Electronic Documents 5
     - 2.2.4 Managing Government Information 5
     - 2.2.5 Retaining Information 6
     - 2.2.6 Ensuring Stewardship 6
   - 2.3 Legislative and Policy Context 6
   - 2.4 General Guidelines 7
   - 2.5 Records and Publications Context 7
     - 2.5.1 Record 7
     - 2.5.2 Government Record 8
     - 2.5.3 Publication 8
     - 2.5.4 Control of Government Information 8
     - 2.5.5 Information Quality 9
     - 2.5.6 Record Description 9
     - 2.5.7 Accounting for the Business Process 9
   - 2.6 Managing Accountability Exposure 10
     - 2.6.1 Accountability 10
     - 2.6.2 Accountability Exposure 10
     - 2.6.3 Risk Management Model 10
     - 2.6.4 Assessing the Level of Risk 12
   - 2.7 Roles and Responsibilities 13
     - 2.7.1 Chief Information Officer 13
     - 2.7.2 Content Managers 14
     - 2.7.3 Records Officers 14
     - 2.7.4 Departmental Librarians 14
     - 2.7.5 Communications Managers 14
     - 2.7.6 Web Administrators 14

2.8 Management Framework 15
2.8.1 Accountability Awareness 15
2.8.2 Accountability Exposure Analysis 15
2.8.3 Accountability Framework 15
2.8.4 Integration with the Record-keeping Function 16
2.8.5 Policies, Standards and Practices 16

3. Record-keeping and Publication Requirements 18
3.1 Record-keeping Requirements 18
3.1.1 Developing Integrated Electronic Record Keeping 18
3.1.2 Carrying Out an Accountability Exposure Analysis 18
3.1.3 Responding to Exposure 19
3.1.4 Establishing Record-keeping Links 20
3.1.5 Managing Static and Interactive (Real-time) Website Postings 20
3.1.6 Segregating the Level of Risk 22
3.2 Description of Web-based Records 22
3.2.1 Description 23
3.2.2 Links to Structured Classification 23
3.2.3 Metadata 23
3.2.4 Document Profiles and Meta Tags 24
3.2.5 Document Profiles 24
3.2.6 Metadata Elements 24
3.2.7 Support for Multiple Views 28
3.3 Publication Requirements and Legal Deposit 28
3.3.1 Mandate of the National Library of Canada 28
3.3.2 Legal Deposit Requirements 29
3.3.3 Identification of Documents for Legal Deposit 29
3.3.4 Exclusions 30
3.3.5 Access to Databases 30
3.3.6 Timing of Deposits 31
3.3.7 Deposit Process 31
3.3.8 Use of Metadata 31
3.3.9 Acceptable Transfer Protocols 32
3.3.10 Technical Requirements 32
3.3.11 Access to the National Library of Canada Depository 33
3.3.12 Migration of Legacy Holdings 33
3.3.13 Enquiries 33
3.3.14 Serial Publications 34
3.3.15 Storage of Current Issues 34
3.3.16 Access to Back Issues 34
3.4 The E-library 34
3.4.1 Definition 34
3.4.2 Access Management 35
3.4.3 Risk of Loss of Access 35

3.4.4 Identification and Selection 36
3.4.5 Bibliographic Access 36
3.4.6 Naming 36
3.4.7 Access to the E-library 36
3.4.8 Preservation for Continuous Public Access 37
3.5 Retention and Disposition of Web-based Records 37
3.5.1 Retention Guidelines and Disposition Requirements 37
3.5.2 Definitions 38
3.5.3 Active Use on the Web 38
3.5.4 Purpose of Retention and Disposition 39
3.5.5 Application 39
3.5.6 Retention and Disposition Under Conditions of Low Risk .. 39
3.5.7 Retention and Disposition Under Conditions of Moderate Risk 40
3.5.8 Retention and Disposition Under Conditions of High Risk 41
3.6 Local Site Repository 42
3.6.1 Definition 42
3.6.2 Limits 43
3.6.3 Use 43
3.6.4 Contents 43
3.6.5 Optional Selective Capture 43
3.6.6 Long-term Access 44
3.6.7 Readability 44
3.6.8 Multi-year Disposition Planning 44
3.6.9 Retention and Disposition Management 44
3.6.10 Repository Management 45
3.7 Backup and Disaster Recovery 46
3.7.1 Backup Procedures 46
3.7.2 Essential Records 46
3.8 Quality Assurance 47
3.8.1 Review Process 47
3.8.2 Review Date 47
3.8.3 Audit Trails 47
3.9 E-mail Messages 48
3.9.1 Electronic Work Environment 48
3.9.2 Chat Rooms and List Servers 48

4. Future Considerations and Emerging Trends 49
4.1 New Business Practices 49
4.2 Document Management 49

Annex A: Application of the Risk Management Model A-1

Annex B: Web Administrator's Checklist B-1

Annex C: Glossary **C-1**

Annex D: References and Authorities **D-1**

1. Executive Summary

This document provides guidelines for implementing the IM Forum's ***Approach to Managing Internet and Intranet Information for Long-term Access and Accountability***. *They are designed to ensure that appropriate levels of management control are put in place to protect government records as evidence of the government's business activities; to reduce the levels of risk associated with managing information within networked facilities; and to provide ongoing access to information for as long as it continues to retain its value.*

The implementation guidelines are strongly rooted in the notion of accountability. They suggest that government institutions that use the Web for business operations are creating records as a result of these activities, and that they need to be aware of their obligation to manage this information.

- **For records** this entails ensuring that records posted to the Web are captured and/or described as evidence in a corporate record keeping system, and managed from creation through disposition in keeping with the intent of the *National Archives of Canada Act (1987)* and the provisions of the Treasury Board Policy on the Management of Government Information Holdings.

- **For published material**, this entails preserving long term access to material which has ongoing value, by depositing it with the National Library at the time of publication, in accordance with the Legal Deposit provisions of the *National Library of Canada Act*; and, where warranted by depositing published material in the departmental library where departmental staff and the public (where appropriate) may have ongoing access to it.

The implementation guide provides a number of suggested tools and best practices to help departments fulfill these requirements. These include the following:

Management framework. Such a framework helps a department integrate its Web posting and management functions within its overall record-keeping and publication management functions by establishing corporate policies, standards and practices and assigning clearly defined roles and responsibilities.

Risk management model. This model looks at the levels of risk associated with managing information on individual Websites and recommends appropriate record-keeping and publication management responses to mitigate that risk. Risk factors include the adequacy of existing management structures, the extent to which the corporate record-keeping system captures posted records, the degree to which Legal Deposit captures publications and the information's potential to generate adverse reaction. Escalating levels of response range from continuing to maintain close integration with the corporate record-keeping system, to maintaining snapshots and developing ancillary "local site repositories."

Publications requirements and Legal Deposit. In keeping with the *National Library of Canada Act*, this guide provides a process for ensuring that all government publications posted to a departmental Website are identified for Legal Deposit. As well, the guide introduces the concept of the departmental e-library as a way of providing long-term access to information that remains valuable long after it is removed from an active Website.

Retention and disposition of records. All records posted to a Website are subject to the requirements of the *National Archives of Canada Act (1987)* and Records Disposition Authorities (RDAs) signed by the National Archivist. Institutions must adhere to archival decisions as reflected in RDAs (including the new Multi-Institutional Disposition Authorities, or MIDAs). However, institutions, *not* the National Archives, are responsible for determining retention periods for records they manage in the conduct of government business. In keeping with the risk management model, this guide provides a variety of implementation practices. These range from disposing of posted Web documents that duplicate information already captured in a record-keeping system and therefore residing on the Web under low-risk conditions, to maintaining and disposing of original Web-based corporate records within a "local site repository" under high-risk conditions.

Local site repository. The guide introduces a relatively new concept - the "local site repository"- as an interim measure for retaining and disposing of Web-based records under high-risk conditions. Using client-server technology, the repository replicates all records at the time they are posted to an active Website and allows institutions to manage that information using metadata.

Metadata. This guide recommends that institutions use metadata to describe information content and context and to manage records and publications throughout their lifecycle. Since numerous initiatives are already underway in this area—including the IM Forum Description Working Group, the Treasury Board of Canada, Secretariat Government Information Locator System (GILS) Working Group, and the Treasury Board of Canada, Secretariat Records and Document Information Management System (RDIMS)—and since library cataloguing practices are well established, the guidelines do not attempt to provide additional metadata standards for the Web. Rather, they speak to the functional requirements that emerge from the guidelines.

While the guidelines urge individual departments to manage Web-based records as an integral part of their overall record-keeping environment, they also recognize that not all government departments have developed the same record-keeping capability. Accordingly, the guidelines suggest that those departments that lack the requisite record-keeping infrastructure implement more rigorous and costly management processes for their Websites in the short run, given the high levels of risk associated with information loss, misinterpretation and misuse. In the long run, better record-keeping practices will reduce these costs while improving the quality of information.

2. Management Framework

2.1 Introduction

2.1.1 Purpose

The following guidelines address the need to manage information made available through the Government of Canada networked facilities. *They are designed to ensure that appropriate levels of management control are put in place to protect government records as evidence of the government's business activities; to reduce the levels of risk associated with managing information within networked facilities; and to provide ongoing access to information for as long as it continues to retain its value*. For the purpose of these guidelines, government networked facilities include the Internet, intranets and extranets, serving both Government of Canada employees and the public.

2.1.2 Background

The increased use of electronic networks—including wide area networks, the Internet, intranets and extranets—has fundamentally changed the way we exchange, use and manage information. Our focus is no longer solely on managing physical objects but rather on managing multiple instances of documents, each of which may satisfy a different purpose. As the environment has changed so too has our ability to maintain the necessary levels of quality, integrity and accountability associated with documents. As well, the lines that once clearly separated the disciplines of record keeping and library science, as well as published material and recorded evidence, may no longer serve the best interests of our clients. More than ever, we need a coordinated approach that combines the strengths of multiple disciplines.

2.1.3 Scope

The guidelines that follow apply to all federal government institutions and address the management of both records and published material on networked facilities, whether for public consumption or for departmental use.

2.2 Information Management Principles

The guidelines in this document are based on the following information management principles.

2.2.1 Supporting Decision Making

Institutions should manage information to support effective decision making, public accountability, cost-effective delivery of programs and services, and public access.[1]

2.2.2 Managing Evidence

All organizations must manage records. Records show how we act; how we deal with our clients, customers, other agencies or bodies in the private sector; and how they deal with us. They are the principal means of demonstrating how we have fulfilled our obligations and, in turn, they hold us accountable for our actions.

2.2.3 Managing Electronic Documents

Managing electronic information is a significant part of the business operations of the Government of Canada. No single medium currently contains all the information relating to an organization's business activities. Therefore, all sources of information must be managed in a coordinated way, in a manner appropriate to their environment, to preserve and provide appropriate access to records that document the government's business activities.

2.2.4 Managing Government Information

Government information in all its forms—including printed materials, voice recordings, electronic data and images—is a strategic resource and should be effectively managed throughout its lifecycle.[2] Accordingly, there is a continuing need:

- to effectively manage both government information and its metadata;
- to establish accountabilities, roles, responsibilities, and service standards for managing information and metadata; and
- to ensure that information is created and stored in a way that supports preservation and ongoing access.

---

1 Treasury Board of Canada, Secretariat, *Information Policy Framework*, June 4, 1996.

2 Treasury Board of Canada, Secretariat, *Blueprint for Renewing Government Services Using Information Technology (Discussion Draft)*, undated, p. 56.

2.2.5 Retaining Information

Government information should be retained *only* when there is a business need, when there is a legislative or policy requirement, or when it has historical or archival importance.[3]

2.2.6 Ensuring Stewardship

Specific organizational units should be accountable for managing designated classes of government information to ensure their integrity, quality and relevance and to restrict their accessibility to authorized users.[4]

2.3 Legislative and Policy Context

The guidelines in this document reflect the requirements of the following:

- the *Access to Information Act*;
- the *Copyright Act*;
- the *National Archives of Canada Act*;
- the *National Library of Canada Act*;
- the *Official Languages Act*;
- the *Privacy Act*;
- the Government Security Policy;
- the Treasury Board of Canada, Secretariat Policy on the Management of Government Information Holdings; and
- the Treasury Board of Canada, Secretariat Policy on the Use of Electronic Networks.

---

[3] *Ibid.*, p. 60.

[4] *Ibid.*, p. 61.

2.4 General Guidelines

In managing records and published material on networked facilities, institutions should follow the following broad guidelines: (detailed guidelines follow).

- **Maintain accountability.** Assign clear accountability for managing all departmental Websites and for managing all information made accessible through those sites.

- **Reduce risk exposure.** Manage departmental Websites in a way that reduces the risk exposure associated with each Website (see section 2.6, "Managing Accountability Exposure").

- **Maintain corporate records.** Capture all records and associated metadata posted to a Website of the Government of Canada in a corporate record-keeping system.

- **Provide long-term access.** Ensure that ongoing access to published material is preserved by depositing published material with the National Library at the time of publication, in accordance with the Legal Deposit provisions of the *National Library of Canada Act*; and, where warranted by depositing published material in the departmental library where departmental staff and the public (where appropriate) may have ongoing access to it.

- **Describe content and context.** Describe all documents posted to departmental Websites in a manner that provides ready access to reliable and authentic records while preserving and making visible their evolving context.

- **Retain and dispose of records properly.** When records are no longer required for use on a departmental Website, dispose of them in accordance with Records Disposition Authorities, taking established retention periods into account.

2.5 Records and Publications Context

The following section describes the context within which records and publications posted to Government of Canada Websites should be managed.

2.5.1 Record

In accordance with the *National Archives of Canada Act (1987)*, "record" includes any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microform, sound recording, videotape, machine-readable record and any other documentary material, regardless of its physical form or characteristics, and any copy thereof.

2.5.2 Government Record

For the purpose of these guidelines and within the context of the definition of "record" in the *National Archives of Canada Act (1987)* and the *Access to Information Act*, a "government record" is recorded information, regardless of its physical form, that a government institution controls and that is collected, created, received or used to initiate, conduct or complete an institutional activity. To meet business and accountability requirements, government records must have sufficient content, context and structure to provide evidence of the activity.[5]

2.5.3 Publication

In accordance with the *National Library of Canada Act*, "published in Canada" means "released in Canada for public distribution or sale, otherwise than by her Majesty in right of a province or municipality." The National Library defines "networked electronic publication" as a "digitally encoded information resource made available to the public through a communication network."[6] The Treasury Board Policy on the Management of Government Information Holdings amplifies these definitions; it states that "published material refers to an information product which has been created and edited for the purpose of distribution or sale. Material published by or for Federal Institutions is deposited in federal library collections."[7] For the purpose of these guidelines, "information products" are documents compiled from available information or data sources that are published for a defined audience and a stated purpose.[8]

2.5.4 Control of Government Information

A record is considered to be *under the control of a government institution* when that institution is authorized to grant or deny access to the record, to direct its use and, subject to the approval of the National Archivist, to dispose of it. Records in the possession or custody of an institution, whether at headquarters, regional, satellite or other offices within or outside Canada, are presumed to be under the control of that institution unless there is strong evidence to the contrary.[9]

---

5 National Archives of Canada, Information Management Standards and Practices Division, *Record Keeping in the Electronic Work Environment—Vision*, 1996, p. 1.

6 National Library of Canada, Electronic Collections Coordinating Group, Networked Electronic Publications Policy and Guidelines, October 1998.

7 Treasury Board of Canada, Secretariat, Policy on the Management of Government Information Holdings, 1994.

8 Health Canada, Records Management Policy, September 1998.

9 National Archives of Canada, *Alternate Service Delivery—Record Keeping Issues and Questions, A Summary Checklist*, August 20, 1998, p. 3.

2.5.5 Information Quality

In managing the quality of recorded information, government departments should ensure that all records and publications under their control are continually assessed with respect to the accuracy, reliability and authenticity of the document *content* as well as the accuracy, reliability and authenticity of the *information about the document*—in other words, the document metadata.

2.5.6 Record Description

In keeping with the above, all government information, including information distributed on the Web, should be described in a manner that:

- **facilitates access**, to provide an effective means of accessing and retrieving information;
- **establishes context**, to ensure that information can be understood within the administrative and operational context within which it was generated;
- **provides evidence**, to support the capture and maintenance of reliable, authentic records ("Reliability refers to the authority and trustworthiness of records as evidence, that is, their ability to stand for the facts they are about. Authenticity refers to the fact that the record is what it purports to be, i.e. that it has not been manipulated, altered, or otherwise falsified after its creation..."[10]); and
- **facilitates preservation**, to ensure that information that needs to be preserved remains understandable and accessible over time.

2.5.7 Accounting for the Business Process

Record descriptions must account for the business processes, and associated actions and transactions, that generated the records; the business function or activity supported by the business processes; and the organizational unit accountable for the business processes and the records.[11]

---

[10] Duranti, L. (University of British Columbia). Extracted from National Archives of Canada, *Approach to the Description and Classification of Government Records*, February 1999, p. 2.

[11] National Archives of Canada, *Approach to the Description and Classification of Government Records*, February 1999, p. 3.

These requirements are good business practice and reduce risks arising from increased liabilities or decreased opportunities that accompany poor record-keeping practices.[12]

2.6 Managing Accountability Exposure

2.6.1 Accountability

Government institutions using the Web for business operations need to be aware that they are creating records as a result of these activities. Organizations, therefore, have an obligation to manage this information the same way they manage any other record or document they create in the conduct of government business. They should keep records containing government information in appropriate record-keeping systems so that they can be protected, accessed and conveniently used.

An accountable manager, who authorizes the posting of a document on an electronic network, is deemed to have certified that:

- the document and its associated metadata are accurate, current and complete, and that they convey authorized direction; and

- the corporate copy of the record and its metadata is being managed in accordance with good record-keeping practices.

2.6.2 Accountability Exposure

In the absence of appropriate management controls, individuals who disseminate information on departmental Websites may be exposing both themselves and the organization to unwarranted levels of risk. The potential costs of "exposure" may include the loss of operationally critical information, increased administrative costs associated with re-creating existing information, non-compliance with relevant legislation and policy, high legal costs associated with responding to evidential claims, declining levels of client satisfaction and the untimely loss of corporate memory.

2.6.3 Risk Management Model

The risk management model looks at the levels of risk associated with managing information on individual Websites and recommends appropriate record-keeping and publication management responses for mitigating that risk. Risk factors include:

---

[12] National Archives of Canada, *Functional Requirements for Record Keeping in the Government of Canada*, undated, p. 2.

- the adequacy of existing management structures;
- the extent to which the corporate record-keeping system captures posted records;
- the degree to which publications are identified for Legal Deposit and deposited in the departmental e-library;
- the volatility of the posted information; and
- the information's potential to generate adverse reaction.

Escalating levels of response range from continuing to maintain close integration with the corporate records-keeping system, to maintaining snapshots and developing ancillary local site repositories. For modelling purposes, the level of "accountability exposure" or potential risk has been divided into three distinct environments, labelled low, moderate and high. Figure 1, "Accountability Exposure Analysis, and Record-keeping and Publication Management Response," describes these environments and their recommended responses. The model is based on the original work of Dr. J. Timothy Sprehe and Dr. Charles R. McClure.[13]

---

[13] For further reading, see *Analysis and Development of Model Quality Guidelines for Electronic Records Management on State and Federal Websites* by Charles R. McClure and J. Timothy Sprehe, January 1998, pp. 7–11, <http://istweb.syr.edu/~mcclure/nhprc/nhprc_chpt_6.html>.

Figure 1: Accountability Exposure Analysis, and Record-keeping and Publication Management Response

Low Risk of Accountability Exposure	Record-keeping and Publication Management Response
• The department effectively controls who may post to Websites and what may be posted. • Websites contain mostly static documents. • There is little or no adverse reaction to posted documents. • The corporate record-keeping system has captured all posted records. • All publications are also disseminated in other formats.	• Continue to maintain close integration with the corporate record-keeping system. • *At the end of the record's life on the Web, dispose of it in accordance with Records Disposition Authorities (RDAs) approved by the National Archivist.* • Continue to identify material for deposit in the National Library and the departmental e-library.
Moderate Risk of Accountability Exposure	**Record-keeping and Publication Management Response**
• Posting controls are inadequate to meet the growing number of sites. • The Website is beginning to host dynamic and interactive documents. • There is growing potential that some posted documents may generate adverse reaction. • Websites sometimes contain original record material that the corporate record-keeping system has not captured. • Some publications have no print equivalents.	• Improve existing levels of integration with the corporate record-keeping system. • Maintain an historical log and capture it within the corporate record-keeping system. • *At the end of the record's life on the Web, dispose of it in accordance with Records Disposition Authorities (RDAs) approved by the National Archivist.* • Continue to identify material for deposit in the National Library and the departmental e-library.
High Risk of Accountability Exposure	**Record-keeping and Publication Management Response**
• Posting controls show evidence of breaking down. • Websites contain a significant quantity of interactive and dynamic material, including bulletin board postings. • Websites are under intense public scrutiny and posted material is beginning to generate negative reaction. • There is clear evidence that the site contains many records that the corporate record-keeping system is not capturing. • Many publications are available only on the Website with no print equivalents.	• Assess the adequacy of the existing corporate record-keeping system and, where necessary, begin to rebuild processes for closely integrating this system with the Web. • Maintain an historical log and transfer it to the corporate record-keeping system. • Maintain snapshots and a site index (where there is an external threat) and transfer these to the corporate record-keeping system. • *Develop and maintain a local site repository as a temporary means of managing the disposition process for both records and published material.* • Use the local site repository to help identify material for deposit in the National Library and the departmental e-library.

2.6.4 Assessing the Level of Risk

In assessing the level of risk and determining the appropriate response, each department should perform an accountability exposure analysis for each of its Websites. Depending on the specific nature of the risk, the department may need to invoke one or more of processes

described in Figure 1 to mitigate existing or potential risk. Sample assessments and responses are shown below. (For an implementation overview, see the diagram in Annex A.)

- *Organization XYZ is fairly confident that its Website management controls are adequate. The corporate record-keeping system is capturing all record material and an effective process is in place to ensure that published information is identified for Legal Deposit and the departmental library. Recently, however, many posted documents have begun to generate enquiries from a concerned public. As well, much of the information content of the posted documents is changing rapidly, and enquiries increasingly concern access to previously posted information. The manager correctly anticipates the trends and begins to create "weekly" snapshots of the site as an effective response mechanism, thereby mitigating potential risk and enhancing overall client service.*

- *Organization ABC has not yet implemented an electronic corporate record keeping system but is in the process of doing so. Under the current arrangement many of the department's publications are available only on the Web. As well many documents posted to the Web are being overwritten with new versions or are being deleted at the end of their active life on the Web. Publications and record material are clearly being lost. The departmental CIO, recognizes this as a high risk situation, and immediately instructs program managers, Web administrators and records manager to develop a "Local Site Repository" strategy to guide the interim management of Web-based records until such time as the corporate record keeping system is deemed adequate to the task.*

2.7 Roles and Responsibilities[14]

Effectively managing records and publications within a Website environment requires the coordinated efforts of a number of key functional areas. In most government departments, these include the Chief Information Officer (CIO), Web administrators (or Website managers), content managers, communications managers, publications managers, records officers and library professionals. Their areas of responsibility are distinguished as follows:

2.7.1 Chief Information Officer

The Chief Information Officer is normally the designated senior information resource manager in the department who is responsible for overseeing and coordinating the department's information management (IM) activities, including activities related to operating and

---

[14] This section is based largely on *Analysis and Development of Model Quality Guidelines for Electronic Records Management on State and Federal Websites* by Charles R. McClure and J. Timothy Sprehe, January 1998, pp. 5–6, <http://istweb.syr.edu/~mcclure/nhprc/nhprc_chpt_6.html>.

managing departmental Websites. The senior official for the management of government information holdings (MGIH) is often the closest recognized role.

2.7.2 Content Managers

Content managers are responsible for creating and managing information content. An accountable content manager should be assigned to each document posted on the Web. Content managers ensure that the content of posted documents and their associated metadata is accurate and complete; that the corporate record-keeping system has captured all record material; and that a departmental e-library has captured original and revised versions of all published material and made them accessible. They are most frequently found in the program offices of departments, engaged in carrying out the programs that comprise departmental missions.

2.7.3 Records Officers

Records officers carry out the department's official record-keeping and archival responsibilities. They ensure that the department creates, maintains, transfers, and disposes of records in accordance with applicable legislation and policy.

2.7.4 Departmental Librarians

Departmental librarians facilitate public access to departmental publications by identifying, cataloguing and storing them. Internet publications should be catalogued and, ideally, stored and made accessible through a departmental e-library. In conjunction with the content manager and the National Library of Canada, departmental librarians also identify publications that need to be deposited in the National Library of Canada.

2.7.5 Communications Managers

Communications managers manage the flow of information to Websites and provide quality control. They often decide when information will be posted, whether the Website should be limited to current information and when information will be removed from the Website. They may decide whether information is appropriate for the Internet or an intranet.

2.7.6 Web Administrators

Web administrators manage the information technology aspects of Websites. In many organizations, Web administrators or their designates operate and maintain Websites, administer the posting rights of content managers and help determine the appropriate format for posted documents, as well as edit, mark up and post the documents. Their role may also include "gate-keeping" to ensure that appropriate metadata are captured and that an accountable content manager has carried out appropriate record-keeping and publication management activities (see Annex B, "Web Administrator's Checklist").

2.8 Management Framework[15]

Departments should have a management framework to provide for the oversight of all functions and activities associated with departmental Websites. The departmental CIO should have overall accountability for the framework. Suggested functions should include the following:

2.8.1 Accountability Awareness

Departmental CIOs should ensure that all staff:

- are made aware of the risks and benefits associated with the use of Websites; and
- understand and comply with legislative and policy requirements governing the management of recorded information under the control of an institution.

2.8.2 Accountability Exposure Analysis

Departmental CIOs should ensure that *all* departmental Websites are assessed with respect to their potential accountability exposure and that there is a certification process to:

- define the level of risk associated with each Website, both at time of installation and periodically over the life of the site; and
- document the required levels of record-keeping intervention needed to mitigate the identified risk.

2.8.3 Accountability Framework

The departmental CIO should establish an overall accountability framework for Website management that:

- **includes Website creation policies and practices** that specify who has the authority to create Websites and under what conditions the legal branch or public affairs specialists should be consulted;

---

[15] This section is based largely on *Analysis and Development of Model Quality Guidelines for Electronic Records Management on State and Federal Websites* by Charles R. McClure and J. Timothy Sprehe, January 1998, pp. 12–13, <http://istweb.syr.edu/~mcclure/nhprc/nhprc_chpt_6.html>.

- **assigns clearly defined roles and responsibilities** for each person involved in managing departmental Websites, including Web administrators, communications managers, content managers, records officers, librarians, publication managers, public affairs specialists and legal counsel;

- **establishes a coordinating mechanism** to ensure that Web administrators, content managers, records officers, librarians and publication managers coordinate their efforts.

2.8.4 Integration with the Record-keeping Function

Departmental CIOs should ensure that Website management functions and activities are incorporated within the overall record keeping and publication management functions of the department.

2.8.5 Policies, Standards and Practices

Departmental CIOs should ensure that corporate policies, standards and practices are developed for managing Websites and that clearly defined roles and responsibilities for discharging these are assigned. Specific activities should include the following:

- **Posting control.** Departments should ensure that only authorized individuals are permitted to post information on departmental Websites.

- **Certification.** Departments should ensure that those who maintain accountability for the information content—that is, content managers—have discharged their record-keeping and publication management responsibilities before releasing a document for posting on the Web.

    - **For static documents**, this includes capturing the source document in the corporate record-keeping system, as well as updating the associated metadata with information relevant to the posting process and, where warranted, identifying and depositing published material in the departmental e-library and the National Library.

    - **For dynamic documents**, this entails ensuring that the record-keeping system has captured significant changes, capturing relevant metadata regarding the posting process and in, cooperation with the departmental librarian, identifying and capturing significant changes to published material in the departmental e-library and the National Library.

    - **For business or service transactions**, this entails capturing those transactions that the department has defined as business activities. (Additional care should be taken when these transactions involve members of the public.)

- **Quality assurance.** Establish control procedures to ensure that all material posted on the Web is systematically assessed for timeliness, relevance and quality, both at the time of posting and periodically thereafter.

- **Version control.** Define criteria, procedures and responsibilities for managing different versions of the same document. This includes defining the conditions under which the organization should maintain various versions of a document.

- **Retention and disposition.** Ensure that the organization has established appropriate retention periods and that it disposes of Website information in accordance with Records Disposition Authorities. As well, when the organization must transfer archival information to the National Archives, ensure that it does so in coordination with the disposition of other departmental information holdings.

3. Record-keeping and Publication Requirements[16]

3.1 Record-keeping Requirements

In applying the overall management framework to departmental Websites, include the following record-keeping requirements:

3.1.1 Developing Integrated Electronic Record Keeping

Departments need an integrated electronic record-keeping system to manage all Website records and all other non-paper-based records, such as electronic mail, word processing documents and optically stored files. That capability should include the following:

- **Department-wide understanding of records and record-keeping requirements.** Departments need to ensure that all employees understand what constitutes a record and why it is important to manage departmental records as a corporate resource.

- **Policies and practices.** Departments need clearly defined record-keeping policies, standards and practices, as well as the resources to carry out assigned record-keeping responsibilities.

- **Tools for managing electronic record content and context.** Departments need to give staff the tools to describe, access and manage electronic records.

3.1.2 Carrying Out an Accountability Exposure Analysis

Carry out an accountability exposure analysis for each Website, in accordance with the following requirements:

- **Exposure analysis.** For each Website, the web administrator, content manager and records officer should jointly determine the site's accountability exposure, seeking advice, where appropriate, from legal counsel and the department's public affairs specialists. Websites may be classified as having low, moderate or high accountability exposure.

- **Determining the response.** The Web administrator, content manager and records officer should jointly determine appropriate record-keeping responses to low, moderate and high accountability exposure sites.

---

[16] The section is largely based on *Analysis and Development of Model Quality Guidelines for Electronic Records Management on State and Federal Websites* by Charles R. McClure and J. Timothy Sprehe, January 1998, pp. 13–14, <http://istweb.syr.edu/~mcclure/nhprc/nhprc_chpt_6.html>.

3.1.3 Responding to Exposure

The following provides suggested record-keeping responses to the existing level of Website accountability exposure (for further information, see Figure 1, "Accountability Exposure Analysis, and Record-keeping and Publication Management Response").

- **Low accountability exposure.** Where the level of accountability exposure is low, institutions should continue to use existing record-keeping policies, standards and practices. They should review the Website periodically to ensure that the levels of exposure have not increased.

- **Moderate accountability exposure.** Where the level of accountability exposure is moderate, organizations should supplement their existing record-keeping policies and practices by *creating and maintaining an historical log for the Website*. The following data elements could be included in the historical log:

  - the title or name of the posting;
  - the version number of the posting;
  - the originating author and his or her office name, address and contact information (this is usually the content manager, or another person or office responsible for creating content);
  - hyperlinks in the posting;
  - the date of the initial posting;
  - the date of the last modification of the posting;
  - the date of the replacement or withdrawal of the posting; and
  - the disposition of the posting after it was replaced or withdrawn.

  The historical log itself is an official record to be transferred to a record-keeping system. Also, post the log on the Website so that users interested in the long-term availability of postings can find information on past postings.

- **High accountability exposure.** Where the level of accountability exposure is high, organizations should supplement those policies and practices suited to low and moderate accountability Websites with the following *additional* safeguards.

- **Create periodic electronic snapshots to enable Website reconstruction.** When an organization needs an exact reconstruction of a Website to respond to potential enquiries quickly—that is, for legal or accountability purposes—they should create procedures for taking an electronic "snapshot" of the entire Website. These snapshots constitute official records, which should be included in the departmental record-keeping system. Snapshots may be taken as often as needed, even daily or hourly. Departments should frequently assess how often they should be taking snapshots.

- **Create local site repositories.** Where existing record-keeping systems are not adequate for managing the retention and disposition of Web-based records, organizations should consider using a local site repository temporarily, until such time as the corporate record-keeping system is deemed adequate (see section 3.6, "Local Site Repository"). The site repository should:

  - replicate, at time of posting, all material posted to the active site;

  - be maintained in a separate repository;

  - provide for the interim management of the record retention and disposition process; and

  - be linked to the departmental classification system through the document metadata.

3.1.4 Establishing Record-keeping Links

When records occur on Websites, organizations should ensure that linkages have been established to departmental record-keeping systems and that the automatic transfer of records to record-keeping systems actually occurs. This includes the need to do the following:

- **Capture posting activities.** For all levels of risk, the activities of posting and removing individual documents from the Web should be captured and associated with the corporate record as part of the overall document context (see section 3.2.3, "Metadata").

3.1.5 Managing Static and Interactive (Real-time) Website Postings

The following section outlines suggested responsibilities for managing static and dynamic Web material:

- **Static material.** For materials prepared in advance for Website posting, the department should establish procedures for capturing records of the materials in record-keeping systems and, where warranted, for depositing published material into the departmental library and the National Library.

  - **Content managers.** The content manager responsible for preparing material for posting should ensure that a copy of the posted "record" and its metadata, as well as any administrative records associated with the posting process, are transferred into a record-keeping system either before or at the time of posting.

  - **Web administrators.** Web administrators should ensure that they are following established record-keeping procedures for capturing static material.

  - **Records officers.** Records officers should help develop procedures for capturing static record material, and confirm that content managers and Web administrators are following the procedures.

  - **Departmental librarians.** Departmental librarians should help develop procedures for capturing static publication material, and confirm that content managers and Web administrators are following the procedures.

- **Dynamic materials.** For materials that appear on department Websites as a result of an interactive, real-time event, departments should assign responsibilities, preferably before the event happens, specifying how the materials will be assessed from a record-keeping standpoint, which program office has record-keeping responsibility for the materials and how the resulting records will be transferred to the corporate record-keeping system. They should also establish follow-up review procedures to ensure that transfers actually occur.

  - **Web administrators.** Web administrators should consult with content managers and records officers to determine whether the materials qualify as records, which program office is responsible for the content of the materials and how the corporate record-keeping system will capture the records.

  - **Content managers.** Content managers should consult with Web administrators and records officers to determine whether the materials qualify as records, which content manager's office has program responsibility for the content of the materials and how the corporate record-keeping system will capture the records.

  - **Records officers.** Records officers should determine, in advance if possible, whether a given interactive, real-time event on a Website is likely to produce or has already produced records. If it produces records, records officers should

ensure that Web administrators and content managers follow established records transfer procedures and that the corporate record-keeping system in fact receives the records.

- **Departmental librarians**. Departmental librarians should determine whether a given interactive real-time event on a Website is likely to produce or has already produced publications that should be captured in the departmental e-library or are subject to Legal Deposit. If it produces such publications, departmental librarians should ensure that Web administrators and content managers follow established procedures to ensure that such publications are transferred to the departmental e-library and to Legal Deposit.

- **Business or service transactions.** Departments should prepare guidelines for managing transactions conducted through government Websites. These should answer the following questions:

  - What constitutes a business or service transaction?

  - What aspects of the transaction need to be captured?

  - How should evidence of the transaction be maintained?

3.1.6 Segregating the Level of Risk

In managing diverse levels of accountability exposure, departments should segregate material on their Websites by level of potential exposure. This will help them provide the appropriate level of record-keeping response.

3.2 Description of Web-based Records

In fulfilling accountability requirements for managing recorded information, organizations should describe all government information, including Web-based information, in a manner that:

- **facilitates access**, making it easy to find and retrieve information;

- **provides authentic and reliable information** that can be used both for its information content and as a way of documenting an action or transaction;

- **provides context**, so that users can understand information within the administrative and operational context within which it was collected, created, received or used; and

- **facilitates preservation**, ensuring that information that needs to be preserved remains understandable and accessible over time.

As well, records description should account for the business processes, and associated actions and transactions, that generated the records; the business function or activity supported by the business processes; and the organizational unit accountable for the business processes and the records.[17]

3.2.1 Description

In meeting these requirements within a Web environment, departments should ensure that Web-based documents and records are described by:

- using structured metadata; and
- providing links to a structured classification system.

Regardless of the method used to describe records, a record-keeping system will be required to ensure that the records are maintained in a manner that ensures their authenticity and reliability for as long as they are needed to meet various business and accountability requirements.

3.2.2 Links to Structured Classification

In accordance with the above, all documents posted to the Internet, an intranet or an extranet should be linked through their metadata to the existing departmental classification system(s).

As well, the retention periods established for Website information inside the institution, and the disposition decisions reflected in RDAs, should be closely linked to the institution's file classification structure (see section 3.5, "Retention and Disposition of Web-based Records").

3.2.3 Metadata

Document metadata, or information about the document, should be used when managing documents on departmental Websites. Organizations can use metadata to:

- provide access, control and context while a document is on the Web;
- assess the document's authenticity;

---

[17] National Archives of Canada, *Approach to the Description and Classification of Government Records*, February 1999, p. 3.

- provide archival context once the document has been removed form the Web; and

- capture the posting and disposition activities associated with the document as an integral part of its lifecycle in order to provide evidence of the business activity.

3.2.4 Document Profiles and Meta Tags

For the purpose of these guidelines, metadata include structured data contained within document profiles, as well as meta tags embedded within structured documents.

In both cases, metadata should be structured so that:

- they can render their descriptive information explicitly;

- people can see them; and

- they can be extracted automatically to add to the information collection and map to the overall information management structure.

3.2.5 Document Profiles

Where the management of electronic records is enabled through the use of an electronic document management system which supports the use of "metadata profiles" (see RDIMS[18]) much of the metadata will already have been captured as an integral part of the record keeping function.

3.2.6 Metadata Elements

The management of local site repositories within individual government departments will require agreement on the use of a standard set of metadata elements both for describing and managing Web information. Until such time as government-wide standards are adopted, individual departments should rely on existing standards or recognized approaches, such as the Government Information Locator System (GILS), Dublin Core or the Treasury Board of Canada, Secretariat Records and Document Information Management System (RDIMS).

---

[18] For a complete list of recommended metadata elements for record keeping within an electronic system see National Archives Information Management Standards and Practices Division Records/Documents/Information Management (RDIM): Integrated Document Management System for the Government of Canada - Request for Proposal (RFP) Software Requirements May 1996, pp. 7-9

Since numerous initiatives, including those mentioned in the previous paragraph, are already underway, this document does not attempt to provide additional metadata standards. *Any reference to specific metadata elements should simply be seen in light of the functionality being supported.* Notwithstanding the above statement, departments should consider the following list of metadata elements as supporting the management of Web-based-records.

Figure 2: Suggested Metadata Elements for Managing Website Records

Metadata Element	Description
Originator	The information resource originator, including the full name or acronym of the originator's government department, division, organization or bureau. *Source: GILS Mandatory.*
Creator	The person(s) or organization(s) primarily responsible for the intellectual content of the resource, such as authors in the case of written documents, and artists, photographers or illustrators in the case of visual resources. *Source: AGLS, Dublin Core +2.*
Record source	Organizational unit(s) that created or last modified the record; this may or may not be the same as the unit named in the "originator" element, which is the unit that created the actual resource. *Source: GILS Mandatory.*
Posting authority	The name and designation of the individual authorized to post the document to the specified network, also known as "the accountable individual" (if different from the originator). *Source: Working Group.*
E-mail	The person to be notified when the date for review has been reached.
Region	The region where the material originated, such as ATL, QUE, ONT, NCR, WST, PAC.
Sector*	The official name of the author's or owner's sector.
Branch*	The official name of the author's or owner's branch.
Directorate*	The official name of the author's or owner's directorate.
For consistency, use the applied name of the originating department or agency given in "Titles of Federal Organizations," published by Treasury Board of Canada, Secretariat.	
Title	A description presented initially to users, independently of other elements, that conveys the most significant aspects of the referenced resource (including the general topic and the specific subject), allowing users to decide on the document's likely relevance. *Source: GILS Mandatory.*
Version number	The version number of the posted document. *Source: GILS.*
Subject	The topic of the resource, typically expressed as keywords or phrases that describe the subject or content of the resource, using controlled vocabularies. *Source: Dublin Core (modified).*
Language of information resource	The language(s) of the resource, described using three-character alpha codes known as MARC codes. *Source: GILS Mandatory.*
Language destination	Location in which the record will be put, based on language (French site or English site). *Source: Acts as proxy for the GILS Mandatory element <Language_of_record>.*
Abstract	A narrative description of the information resource that allows the user to determine whether the resource has sufficient potential to warrant contacting the provider for further information. *Source: GILS Optional.*

Classification	The classification system identifier used within a department for record-keeping purposes, which should be sufficiently detailed to help the department follow applicable retention and disposition guidelines. *Source: Working Group.*
Date of last modification	The date on which the record was created or last modified, given using the ISO date standard YYYYMMDD (for example, November 21, 1999 would be 19991121). *Source: GILS Mandatory.*
Date of publication	The date on which the information resource was published, posted or updated, depending on its format (**for Web pages, the date posted**; for other information resources, the date the resource was made available via traditional publishing or other means). *Source: GILS Optional.* *Note: Use the ISO date standard YYYYMMDD (for example, November 21, 1999 would be 19991121). If describing a formal publication, use the date on which it was officially released to the public.*
Availability	A description of the medium of the resource—such as cassette, kit, computer database or computer file—which must include a comprehensive list if the medium is not on the Internet and therefore cannot be described using MIME content types. *Source: GILS Optional.*
Date for review	The date on which the department should review the timeliness and relevance of the document and update, delete or transfer the record, given using the ISO date standard YYYYMMDD (for example, November 21, 1999 would be 19991121).
Date of removal	The date on which the document was removed from the active Website, given using the ISO date standard YYYYMMDD (for example, November 21, 1999 would be 19991121).
Removal authority	The name and designation of the individual authorized to remove the document from the Website, if this differs from the posting authority. *Source: Working Group.*
Records disposition authority number	The number assigned by the National Archives to Records Disposition Authorities approved by the National Archivist of Canada. *Source: GILS Optional.* *Note: Associate disposition elements with the classification number or, in the absence of classification, directly with the disposition authority.*
Retention period	The length of time, as determined by the originating institution, that the institution needs to retain the records for operational or legal reasons. *Source: GILS Optional.*
Disposition action	The disposition action approved by the National Archivist, which occurs at the expiry of the retention period. *Source: Adapted from GILS Optional.*
Disposition date	Date on which the retention period expires and the approved disposition action takes place, given using the ISO date standard YYYYMMDD (for example, November 21, 1999 would be 19991121). *Source: GILS Optional.*

Deposit	The name of the repository and the date of deposit; for example, <META NAME="Deposit" CONTENT="NLC-BNC YYYYMMDD." *Source: GILS Optional.*
Software and hardware	The name, version, update and date of update of software; platform information for hardware; and related information. *Source: RDIMS.*
Resource identifier	A string or number used to uniquely identify the resource, such as URLs and URNs (when implemented) for networked resources, international standard book numbers (ISBNs) for printed documents, or other formal names. *Source: Dublin Core.*
Program record	The Access to Information locator number, as given in INFOSOURCE.
Personal information bank	Personal Information Bank Number, as given in INFOSOURCE.

3.2.7 Support for Multiple Views

While a core set of metadata elements may be useful to most Web users and for most functions, departments may also wish to provide audience-specific views in the interests of efficiency, security and ease of access. Departments will need to assess client needs to determine which subsets of internal and external clients require which set of metadata elements. For example, departments may not want to distribute the name of the document creator on the Internet.

3.3 Publication Requirements and Legal Deposit

The following section sets out the requirements for managing publications in relation to Legal Deposit in the National Library of Canada.

3.3.1 Mandate of the National Library of Canada

The National Library collects, preserves and ensures access to Canada's published heritage. The primary process for fulfilling this mandate is Legal Deposit, through which all works published in Canada become part of the National Library of Canada's collections and are made available to Canadians now and in the future.

In accordance with the *National Library Act*, all Canadian publishers, including the Government of Canada and all its departments and agencies, are required to deposit copies of their works with the National Library of Canada.

3.3.2 Legal Deposit Requirements

All government publications posted to a departmental Website should be deposited with the National Library of Canada in accordance with the following guidelines. These guidelines and supporting criteria will be reviewed periodically to reflect changes in collecting priorities and relevant developments in the rapidly changing world of electronic publishing.

3.3.3 Identification of Documents for Legal Deposit

In accordance with the current policy of the National Library of Canada, documents intended for Legal Deposit are normally identified through two avenues:

- when individual departments follow guidelines provided by the National Library of Canada; or
- when the National Library identifies existing titles it wishes to acquire.

When a department has previously published a networked publication in another format, and the networked version contains no enhanced information content or functionality when compared to the original version, the department need not deposit the networked publication. The National Library of Canada may, however, request deposit of the electronic version of key documents, such as parliamentary papers and budget documents.

In general, when the following categories of publication are made available to the public through a communication network, they should be deposited with the National Library of Canada:

- annuals
- annual reports
- bibliographies
- briefs
- conference proceedings
- directories
- fact sheets
- handbooks
- indexes
- market studies
- monographs (books)
- musical recordings
- newsletters
- periodicals and other serial publications
- recorded books
- research reports
- technical reports
- working papers made available to the public.

All editions or versions made available to the public should be dated and deposited. The National Library of Canada will provide access to outdated or superceded versions for historical or accountability purposes. The frequency of selection of new versions or editions of dynamic, frequently changing publications will be determined by discussion on an individual basis. The selection may vary from comprehensive to representative.

3.3.4 Exclusions

The following categories of publication are excluded from deposit at this time:

- biography vignettes
- calendars of days and months
- daily weather charts, if cumulated weekly
- weekly weather charts, if cumulated monthly
- forms, such as tax forms and instructions for completing a form
- games
- guest books
- internal newsletters, including all newsletters or bulletins intended to keep employees informed of events in their department
- letters
- maps
- OPAC (online public access library catalogue)
- mathematical tables used for calculations, such as income tax tables
- plant growing charts that include mostly figures
- promotional sites and advertising materials
- prospectuses
- publications of local organizations, such as union locals
- speeches
- telephone directories of individual government departments
- timetables
- incomplete publications, such as works in progress, drafts, pre-prints, non-official versions or editions, and abridgments (such as selected articles or chapters, abstracts and tables of contents)
- service sites (Web sites that list links for the purpose of organizing Internet information)
- hypertext-linked, open, highly distributed documents ("open" documents contain links to other sources not under the control of the author, as opposed to "closed" documents, where the links point to items located at the same source; open documents consisting primarily of pointers to other network locations are not physically depositable because their integrity cannot be preserved for the future).

3.3.5 Access to Databases

The National Library of Canada does not require departments to deposit Websites per se. The Library will not collect certain information products until its technical environment is altered to properly acquire and store such products. This limitation applies primarily to databases. However, in lieu of current deposit, departments should give the National Library of Canada free access (user ID and password or IP access) to items that it cannot collect at present.

3.3.6 Timing of Deposits

When required to deposit a document, departments should deposit copies of new postings or substantial revisions with the National Library:

- at the time of posting, or
- in accordance with a schedule agreed to with the National Library.

3.3.7 Deposit Process

The following deposit process is recommended:

- The National Library of Canada issues guidelines to departments.
- In the Government Information Locator System (GILS) record for a new electronic resource, a department identifies the resource as subject to deposit.
- The department regularly searches departmental GILS metadata to identify new titles to be deposited—that is, titles subject to deposit posted or published since the last deposit date. The department and the National Library of Canada agree to a schedule for these searches, based on the volume and frequency of departmental electronic publishing.
- The department sends the resources to the National Library of Canada via e-mail or file transfer protocol (FTP), depositing the documents in an assigned FTP directory.
- The department updates the GILS metadata record(s) to indicate that it has deposited the title with the National Library, and the date of deposit.
- The National Library of Canada receives the resource and accompanying metadata and processes them.
- The National Library of Canada makes the resource available on the Internet in its Electronic Collection.
- Using available metadata, the National Library of Canada catalogues the title in its AMICUS database in MARC format and makes it available on the Web via resAnet.

3.3.8 Use of Metadata

The status and location of all publications under the control of a government department should be reflected in the document metadata associated with each publication. Certain metadata elements identified in section 3.2.6, "Metadata Elements," are important to

managing the deposit process. As a minimum, metadata elements should include the following:

- the name of the originating department or agency;
- the title of the publication;
- the date of publication;
- information on whether the publication is subject to Legal Deposit or to some other repository; and
- the actual date and location of the transfer.

A department can use the "Deposit" element of the GILS metadata set for these purposes. When a publication has been updated, the cross reference element can be used to provide a link to previous versions.

Additional metadata elements that reinforce the authenticity of publications and support preservation and long-term access through the National Library of Canada depository include:

- a resource identifier, such as an ISBN or catalogue number; and
- information on software and hardware dependencies.

3.3.9 Acceptable Transfer Protocols

The Library offers several methods for sending files: e-mail, FTP, mirroring, diskette, CD-ROM, and tape. Usage statistics are also available.

3.3.10 Technical Requirements

To make it possible to archive an HTML publication, a department must make sure that the document is easy to transfer and that it will operate on another server. To do this, departments should ensure that:

- all files and subdirectories are contained in one directory;
- relative URLs are used for links inside the publication (e.g.../../images/tree.gif or tree.gif or images/tree.gif or page.html); and
- absolute URLs (e.g...http://www.nlc-bnc.ca) are used for links outside the publication.

3.3.11 Access to the National Library of Canada Depository

Publications deposited with the National Library of Canada are preserved and made available for consultation and research at the Library's Website at <http://collection.nlc-bnc.ca/e-coll-e/index-e.htm>.

Electronic publications are catalogued and bibliographic records are added to AMICUS, the database of bibliographic records. Once catalogued, electronic publications are available through resAnet at <http://www.amicus.nlc-bnc.ca/wapp/resanet/searche.htm>.

ResAnet is a Web-based interface to the National Library of Canada's catalogue. A subset of the AMICUS database, resAnet provides free access to brief records describing the National Library's collections.

The National Library will include the documents in its Electronic Collection, which can serve as the archive or backfile for a department; in other words, the department can retain current issues on its own site, but point users to the Electronic Collection for back issues. For an example of this sort of use, see the Public Accounts on the Public Works and Government Services Canada Website at <http://w3.pwgsc.gc.ca/text/pubacc-e.html>.

3.3.12 Migration of Legacy Holdings

Networked electronic publications held by the National Library of Canada will be migrated and maintained to preserve access for users operating within diverse computing environments.

3.3.13 Enquiries

For more information on the National Library's Electronic Collection, contact the following office:

National Library of Canada
Legal Deposit Division
Electronic Publications
Acquisitions Section
395 Wellington Street
Ottawa, Ontario
K1A 0N4
Telephone: (819) 997-9565
Fax: (819) 953-8508
e-mail: e.publications.e@nlc-bnc.ca

3.3.14 Serial Publications

When a department regularly posts documents to its Internet site in a publication series (such as news releases, issues of a periodical and monthly "what's new" documents), it should use the following structure:

- current issue;
- back issues or archive.

The URLs for both should be kept consistent.

3.3.15 Storage of Current Issues

Current issues should be stored on an active intranet or Internet server.

3.3.16 Access to Back Issues

The department should provide transparent access to back issues or archives through URL links to:

- **the National Library of Canada's Electronic Collection** for all publications deposited with the National Library (see section 3.3.3, "Identification of Documents for Legal Deposit"); or
- **a departmental repository** for back issues of other publications (see section 3.4, "The E-library").

3.4 The E-library

Where they need to provide long-term access to published material that is no longer supported by the active Website, departments may establish a departmental e-library. The e-library would be managed by the departmental library and served by professional staff with expertise in selecting and organizing information, and providing information services. It would give departmental staff and the public (where appropriate) ongoing bibliographic access to electronically published material.

3.4.1 Definition

An e-library encompasses the functions of selection, bibliographic control, electronic storage, access, service and preservation. Publications stored on the e-library's server can be linked to records in a public access catalogue (online or Web based) and made available to users.

The server may be an Internet server managed by the departmental library, part of a departmental Internet server or part of an integrated library system. Departments unable to establish an e-library server may chose to preserve and maintain access to publications through other means, which may include print surrogates.

3.4.2 Access Management

Use of an e-library is in keeping with two management of government information holdings (MGIH) principles: that institutions should "make the widest possible use of information within the government by ensuring that it is organized to facilitate access by those who require it, subject to the legal and policy constraints"[19] and that they should ensure "that all material published by the institution is easily accessible to decision makers within the institution and is available to the public on request."[20] It is also consistent with the principle that "institutions should manage government information holdings in a manner to make it easier for the public to know about, and [provide] access to, such holdings consistent with the principles in section 2 of the *Access to Information Act.*"[21]

In keeping with these overriding principles, this guide should not be seen as limiting in any way access to the type of information normally available to the general public. Existing procedures ensure that publications in print and other tangible formats remain available to the public. Government institutions should look at ways of extending these procedures to electronic publications that are made available on the Internet.

3.4.3 Risk of Loss of Access

The fact that multiple copies of tangible publications are available in multiple libraries minimizes the risk of loss of access. However, networked electronic publications can be made widely available on the Internet from a single copy, and publications are posted on and removed from the Internet in the context of short-term communications needs. These two factors increase the risk of loss of access. Departments should apply existing library science principles and processes to networked electronic publications and, in some cases, develop new processes to minimize this risk.

---

19 Treasury Board of Canada, Secretariat, Policy on the Management of Government Information Holdings, 1994, p. 1.

20 *Ibid.*, section 5.

21 *Ibid.*, Appendix E, section 12.

3.4.4 Identification and Selection

The departmental library selects material for the e-library. Departmental libraries should review their existing collection development policies or selection criteria for departmental publications to see how they apply in the Internet/intranet environment. When the department posts new or significantly revised publications that meet library selection criteria, the departmental library may identify them, or a content manager, communications officer or Web administrator may alert the library. As well as selecting publications for the e-library, the departmental library may also identify publications for deposit with the National Library, when it makes good business sense to do so. The content manager or Web administrator should create metadata that trigger this identification and deposit process (in particular, by using the "deposit" element in GILS). The selection process may involve checking the availability of a publication in another format, such as print, or its inclusion in the departmental records management system. *Duplication between the e-library and the records management system should be minimized but may be justified to continue public access.*

3.4.5 Bibliographic Access

The departmental library should enhance information captured in the e-library by creating a cataloguing record or by using one already created by the National Library, where available. Normally, the cataloguing record should be included in the library's public access catalogue (online or Web based) and reported to the National Library Union Catalogue. The cataloguing record should include URL links to the full text of the publication on the departmental Website, in the departmental e-library or in the National Library of Canada's Electronic Collection. The URL that is the most persistent—that is, the URL least likely to change—should be used in the links, and at least one URL should be maintained over time.

3.4.6 Naming

Ideally, a unique identifier should be established for each publication that will serve as a key to multiple instances of the electronic publication. Until the National Library adopts a persistent naming standard for use in the federal government, URLs must serve the dual purpose of naming and locating Internet information resources. Websites should be managed to minimize changes in URLs of publications. E-libraries and the National Library's Electronic Collection should be managed so that URLs are persistent. (The National Library may establish and manage a central PURL service to help meet this objective.)

3.4.7 Access to the E-library

The department's public access catalogue (online or Web based) would provide primary access to the e-library. Alternate means of direct access via Web pages may also be considered. As a minimum, departmental staff should have onsite access in the departmental library. Ideally, staff could get access to the e-library remotely through an intranet.

The most effective means of making materials in the e-library readily available to members of the public with Internet access is by providing remote Internet access to the e-library. The library should ensure that publications can also be provided to members of the public who do not have Internet access or who require alternate formats. The department may make arrangements with the National Library or depository libraries to provide this service. At minimum, the library should provide onsite access through a public access terminal in the library. Where warranted, the library may also provide access remotely through the Internet. When access is extended to the public, departments should ensure that designated portions of the e-library—such as those containing intranet publications or publications in process—are suitably restricted to departmental or government employees.

3.4.8 Preservation for Continuous Public Access

The e-library should be an authoritative source for departmental electronic publications. The library must verify the completeness of a publication and verify the metadata when adding a publication to the e-library. It should retain all versions of a publication and identify them in the metadata, cataloguing record and a unique identifier, when one is developed. Not all formats need be retained. The library should prefer standard formats for documents retained in the e-library and should encourage the department to create publications in standard formats. The e-library server should be backed up regularly. Archival copies of the electronic collection should be made and stored offsite.

3.5 Retention and Disposition of Web-based Records

The following section outlines the requirements for managing the retention and disposition of Web-based records and suggests disposition strategies to be applied under conditions of low, moderate and high risk.

3.5.1 Retention Guidelines and Disposition Requirements

All records posted to a Website are subject to the requirements of the *National Archives of Canada Act (1987)* and Records Disposition Authorities (RDAs) signed by the National Archivist. Government institutions must adhere to archival decisions reflected in RDAs, including the new Multi-Institutional Disposition Authorities (MIDAs). However, individual institutions—not the National Archives—determine retention periods for the records they manage in the conduct of government business.

3.5.2 Definitions

Within the context of these requirements, the following definitions apply:

- **Disposition.** Disposition is the analysis and appraisal of records under the National Archives of Canada Act.[22] It may result in the destruction of government records, the alienation of records from the control of the government, or the transfer of records with archival or historical importance to the National Archives, by any means and at any time.[23] (See the definition of disposition in the Annex C. For further information on retention and disposition, organizations should consult their records office or the National Archives.)

- **Retention period.**[24] The retention period is the length of time assigned by the originating institution that indicates how long the institution needs to retain the record for operational or legal reasons.

3.5.3 Active Use on the Web

The institution also needs to make a clear distinction between how long information is to be retained for *use on the active Website* and how long the institution *needs to retain the information for operational or legal reasons*.

While the decision to remove information from a Website should be well documented for accountability purposes, most of the text that follows refers to the retention and authorized disposition of records as evidence of a department's business activity, once the decision has been made to remove them from the active site.

---

[22] Under section 5(1) of the *National Archives of Canada Act (1987)*, "no record under the control of a government institution and no ministerial record, whether or not it is surplus property of a government institution, shall be destroyed or disposed of without the consent of the Archivist."

[23] Under Section 4(1) of the *National Archives of Canada Act (1987)*, the National Archives of Canada has the mandate to "conserve private and public *records* of national significance and facilitate access thereto, to be the permanent repository of records of government institutions and of ministerial records, to facilitate the management of records of government institutions and of ministerial records, and to encourage archival activities and the archival community."

[24] As part of the accountability process, all institutions subject to the *National Archives of Canada Act (1987)* must develop retention periods for common administrative records and operational/medium-specific records that apply to their specific institutions, based on their legal mandate and functions, as well as risk analysis and best practices.

3.5.4 Purpose of Retention and Disposition

Accordingly, institutions carry out retention and disposition in a Web-based environment to ensure that they dispose of all records that have reached the end of their retention period in accordance with Records Disposition Authorities signed by the National Archivist.

3.5.5 Application

Departments should retain and dispose of government records through the departmental record-keeping system (manual or electronic). This will ensure that the decision to keep or destroy records is:

- in keeping with approved departmental retention and disposition guidelines, which are normally linked to departmental business activities through the corporate classification structure; and

- controlled by authorized disposition authorities.

Even though costs of storage are declining, institutions should apply retention and disposition procedures as early as possible to ensure that they do not lose records of archival value as a result of poor record-keeping practices or obsolete and inaccessible media, and that they retain information only when a business, legislative or policy requirement exists.

3.5.6 Retention and Disposition Under Conditions of Low Risk

Where the source record has already been captured in the corporate record-keeping system, the Web document may be treated as duplicate information and disposed of when it no longer serves its intended purpose on the active Website.

A Website is operating under low-risk conditions (see Figure 1, "Accountability Exposure Analysis, and Record-keeping and Publication Management Response," for further details) when the posting of information on the Website is adequately controlled and monitored. The corporate record-keeping system routinely captures all records posted on the Website and the information on the site is unlikely to generate adverse reaction from its intended audience. As well, the institution routinely identifies and deposits all publications with the National Library.

When removing documents from the Web under these conditions, take the following actions:.

- Confirm, through the document metadata, that the corporate record-keeping system has already captured the document.

- Where the document has *not* already been captured, ask the accountable content manager to ensure that the corporate record-keeping system captures a *copy* of the document.

- *As much as possible, retain the document in its native format. When there is any question of altering the native format, the Web administrator should request a suitable copy of the source document from the originator.*

- Confirm whether the document is also subject to Legal Deposit and whether such a transfer has already taken place.

  - If the document is suited for Legal Deposit but deposit has not yet taken place, update the metadata of the source record to reflect its status and place a *copy* of the record in a temporary repository for eventual deposit in the National Library (see section 3.3, "Publication Requirements and Legal Deposit").

- Once the document has been captured in the record-keeping system and Legal Deposit requirements have been satisfied:

  - tag the document for removal from the Web;

  - update the metadata in the corporate record-keeping system to reflect the document's transfer and planned destruction;

  - download the document by a specified *date* to a temporary storage medium, ensuring that the document has a unique identifier for retrieval and audit purposes; and

  - retain the document for six months, then *completely* destroy the batched files, by time period.

3.5.7 Retention and Disposition Under Conditions of Moderate Risk

Where the risk of accountability exposure is moderate—as a result of problems stemming from increasing span of control, substantial variability in the capture of records and potential adverse public reaction to some of the posted materials (see Figure 1, "Accountability Exposure Analysis, and Record-keeping and Publication Management Response," for details)—take the following actions:

- Establish an historical log of all material posted on the Website. The historical log provides evidence of the business activity and should:

  - provide sufficient detail to allow users to retrieve the previously published document from source documents;

- be posted on the Website to answer public enquiries about past Website postings; and

- be transferred to the corporate record-keeping system and brought under the records schedule.

- Once the historical log has been transferred treat the Web copy of the posted document as a duplicate of information already captured in a record-keeping system and dispose of it when it no longer serves its intended purpose on the active Website, in a manner similar to that applied under low risk conditions.

3.5.8 Retention and Disposition Under Conditions of High Risk

Where the risk of accountability exposure is high (see Figure 1, "Accountability Exposure Analysis, and Record-keeping and Publication Management Response," for more details)—as a result of increasing Website complexity, an increasing span of control, increasing use of dynamic and interactive Web postings, strong evidence that the corporate record-keeping system is *not* capturing documents and substantial potential for liability stemming from ongoing public scrutiny—take the following actions:

- Continue to maintain basic Website records, as specified for conditions of low risk.

- Maintain an historical log or similar response, as specified for conditions of moderate risk.

- Enable Website reconstruction. *When precise reconstruction of an exact copy of past Website contents is required for accountability purposes*—in other words, to generate timely and precise responses to enquiries—departments should take the following actions:

  - Take periodic snapshots. Departments should take periodic "snapshots" or electronic copies of entire Websites so that they can reproduce entire site contents exactly as they appeared. Periodically, they should re-assess how frequently (hourly, daily, weekly and so forth) they take these snapshots.

  - Maintain Website indices. Departments should maintain comprehensive indices of Website contents over time.

  - Transfer snapshots to the record-keeping system. Snapshots are official records, which should be transferred to the corporate record-keeping system and brought under records schedules.

- Maintain a local site repository. *Where high-risk conditions exist because there are no strong links between the electronic network and the corporate record-keeping system*, departments should *temporarily* use a local site repository to control the disposal of information no longer required on the active Website, until the corporate record-keeping system is deemed adequate for the task. All material and metadata posted on the active site is mirrored or replicated onto the local site repository (see section 3.6, "Local Site Repository"). In addition, departments should use the local site repository to:

    - regularly dispose of all non-archival material, in keeping with departmental retention guidelines and approved records disposition authorities issued by the National Archives;

    - identify and schedule the transfer of archival records to the National Archives;

    - deposit material with ongoing corporate value in a departmental e-library to permit ongoing access by departmental staff and the public, when appropriate; and

    - deposit designated material to Legal Deposit at the National Library (see section 3.3, "Publication Requirements and Legal Deposit").

3.6 Local Site Repository

The following section outlines the requirements for a local site repository to store and manage Web-based records temporarily under conditions of high risk, until the corporate record-keeping system is adequate for the task.

3.6.1 Definition

A local site repository is an electronic repository established by a department to manage copies of that department's electronically recorded information as corporate records. A local site repository is intended to replicate, at time of posting, all material posted on an active Website. Contained in a separate storage device, a local site repository:

- provides a means of reconstructing the information content of an active Website; and

- helps a department dispose of recorded information through:

    - controlled deletion,

    - transfer of archival records to the National Archives (in the case of record material),

- the identification of publications for Legal Deposit (in the case of published material), and

- the identification and replication of material of ongoing informational value required to support a departmental e-library.

3.6.2 Limits

A local site repository is not a backup or snapshot of the active Website. It must be backed up in accordance with the institution's standard backup procedures for managed data. It also does not replace an electronic document and records management system (EDRMS), which remains the recommended method for managing electronic records.

3.6.3 Use

Individual organizations should consider using a local site repository as a temporary means of mitigating risk caused by the absence of strong links between the Website and the corporate record-keeping system.

The local site repository is a stop-gap method. It is not the preferred method for managing Web-based records or their legal disposition. Full integration between a Website and the corporate record-keeping system is still the preferred way to minimize risk.

3.6.4 Contents

A local site repository should contain a copy of *all records* that have been posted on the active Website. It should not contain copies of formal publications that have already been captured in the existing record-keeping system or the publication management system, such as official publications with ISBNs.

Where there is any doubt regarding whether the information has already been captured, include the material in the repository and schedule retention and disposition in accordance with departmental guidelines.

Where information is intended to serve multiple functions—such as record keeping, reference or Legal Deposit—across multiple domains, departments should *duplicate* material rather than risk inadvertently destroying electronically recorded information that has ongoing value.

3.6.5 Optional Selective Capture

Where the levels of risk are manageable, organizations may opt to maintain in their local site repositories only those records that have not otherwise been captured in the corporate record-keeping system. This is an implementation issue dictated by individual operational considerations, including the size and complexity of the Website. When selecting this option,

organizations should ensure that Legal Deposit and e-library requirements are met when the material is posted on the active site.

3.6.6 Long-term Access

Electronically recorded information with ongoing corporate value should be copied (with its metadata) from the *local site repository* and transferred to the departmental library for:

- ongoing access by departmental staff; and
- deposit with Legal Deposit at the National Library, when required.

Departments should consider using automated Web tools, such as spiders or crawlers, to tag and copy material of ongoing reference value.

3.6.7 Readability

Departments should ensure that information stored in a local site repository is readable for as long as the department maintains custody and control of the document.

3.6.8 Multi-year Disposition Planning

Electronic records, like all government records, are subject to legal statutes, including the *Access to Information Act*, the *Privacy Act* and the *National Archives of Canada Act (1987)*. As such, they are to be included in submissions made to the National Archives for disposition authority.

Staff involved in record keeping and information management need to work together to manage electronic records in accordance with corporate and legislative priorities.

3.6.9 Retention and Disposition Management

In a high-risk environment, institutions can manage the retention and disposition of recorded information in a local site repository by using a retention strategy based on metadata captured at time of posting. Critical metadata for this process include:

- the classification system identifier;
- the records disposition authority number;[25]

---

[25] When a disposition authority number has not yet been assigned, users should indicate that disposition authority is "pending." Disposition cannot proceed without a disposition authority.

- the retention period, given using the ISO date standard of YYYYMMDD;
- the date last modified (that is, the posting date), given using the ISO date standard of YYYYMMDD; and
- a pre-established disposition action, such as "destroy" or "transfer to the National Archives."

When records reach the end of their retention period, an institution may dispose of them in accordance with Records Disposition Authorities (RDAs) signed by the National Archivist. At this point in time, records designated as archival may be transferred to the National Archives. Records which do not have archival value and for which there is a valid RDA may be disposed of at the discretion of the creating institution within the context of relevant legislation and business practices.

Accordingly, records that have reached the end of their retention period should be reviewed by the designated content manager before final disposition action.

Departments should ensure that material on the active Website does not outlive its counterpart in the local site repository.

3.6.10 Repository Management

In managing the metadata required for the local site repository, the Web administrator should take the following actions at the time of posting:

- They should confirm with local records management staff and posting authorities that all necessary metadata have been captured.
- *When organizations opt to capture only those records that have not been captured in the corporate record-keeping system,* Web administrators should confirm with local records management staff that the document has already been captured in another medium.
    - When such capture has already taken place, determine whether there is a record-keeping requirement to store a copy of the Web record in the local site repository. There may be no need, since the corporate record-keeping system is already controlling retention and disposition for the other media.
    - When the record has not previously been captured, assign a departmental classification number to the document and transfer a copy of the record to the local site repository at time of posting.

- Ask the departmental library whether the document is a formal publication that has an ISBN or other formal indicator. Formal publications need not be classified or transferred to the local site repository.

- Ask the posting authority whether the document is suitable for Legal Deposit and whether the deposit metadata element has been completed.

- In conjunction with the posting authority, determine whether the document has ongoing reference value—that is, whether it should be copied to the department's e-library—and when such a transfer should take place.

3.7 Backup and Disaster Recovery

3.7.1 Backup Procedures

To protect electronic records from disasters and equipment malfunctions, all Websites and associated repositories, including the local site repository and the e-library, should be backed up regularly in accordance with the institution's standard backup procedures for managed data. Institutions should consider the following best practices.

- A "three generations" backup rule should be applied in which the three most recent backup disks or tapes are kept at all times and the oldest backup copy is used for making a new backup copy.

- Backup disks or tapes should be stored in a safe location away from the office—at minimum, in another building.

- Periodic backup of online data resources is distinct from preservation.

3.7.2 Essential Records

Organizations should also consult their record-keeping staff for essential record requirements under business resumption planning and essential records procedures.[26]

---

[26] For further information, consult the *Emergency Preparedness Act of Canada (1988)* and Treasury Board of Canada, Secretariat, *Business Resumption Planning*, 1992.

3.8 Quality Assurance

Organizations should periodically review all information posted on the Web to maintain a consistent level of information quality, timeliness and relevance.

3.8.1 Review Process

To maintain consistent quality, organizations should consider the following questions:

- Have procedures been put in place to periodically review the posted document for continued accuracy and relevance?
- Has the posted document exceeded the retention period of its source document?
- Have other documents been posted that obscure, supersede or contradict the information provided by the posted document? (Such related documents may not be under the organization's control.)
- Are the document links still current?

3.8.2 Review Date

All information published on a Website should include a review date, placed according to an approved design standard. This date should be based on the expected useful lifetime of the information on the Website.

On the review date, the organization should review the posted document and update it, if necessary, or remove it from the Website.

The review date should not exceed the disposition date of the source record. This ensures that the record copy on the network does not "outlive" the corporate record.

3.8.3 Audit Trails

Departments should maintain an audit trail or history record of all changes made to their Websites. This will help them answer any enquiries related to information on former Web pages. As a minimum, this history should document:

- specific changes made and the reasons why;
- the person who signed off the document, and the date of sign-off; and
- previous and new version numbers.

3.9 E-mail Messages

E-mail and attachments communicated via a Website are records of action. Even though they may be transmitted to the desktop of a departmental official, or stored in a file server or directory dedicated to a specific group, the record-keeping system should capture a copy of the e-mail and its attachment, using established departmental policies and practices.[27]

3.9.1 Electronic Work Environment

For information on handling e-mail messages in networked environments, departments should consult *Managing Electronic Records in an Electronic Work Environment*, published by the National Archives of Canada, Information Management Standards and Practices Division (May 1996). An electronic version of this document can be found on the IM Forum Website under National Archives—Management of Government Records—Products List at <http://www.imforumgi.gc.ca/refer_e.html>.

3.9.2 Chat Rooms and List Servers

When setting up a list server and or chat room on a specific topic, departments should consider assigning a records classification system identifier to the topic. This identifier can then be automatically and transparently applied to all new information generated within the defined space. This approach should help organizations capture record material and permit the organized retention and disposition of the information.

---

[27] National Archives of Canada, *Networked Electronic Information, Perspective of the National Archives and the National Library (Draft)*, December 1997, p. 6.

4. Future Considerations and Emerging Trends

4.1 New Business Practices

The Internet continues to evolve and grow at an exponential rate. The rapid introduction of new business practices and associated technologies is affecting a growing number of Internet users. The merging of computing, telecommunications and broadcasting areas and the development of new technologies, such as "Web TV," is rapidly leading to ubiquitous use of the World Wide Web.

To ensure that departments and agencies maximize the benefits of the Internet, and that departmental Websites remain appropriate, a concerted effort to monitor emerging trends is required. Some examples of these trends are described below.

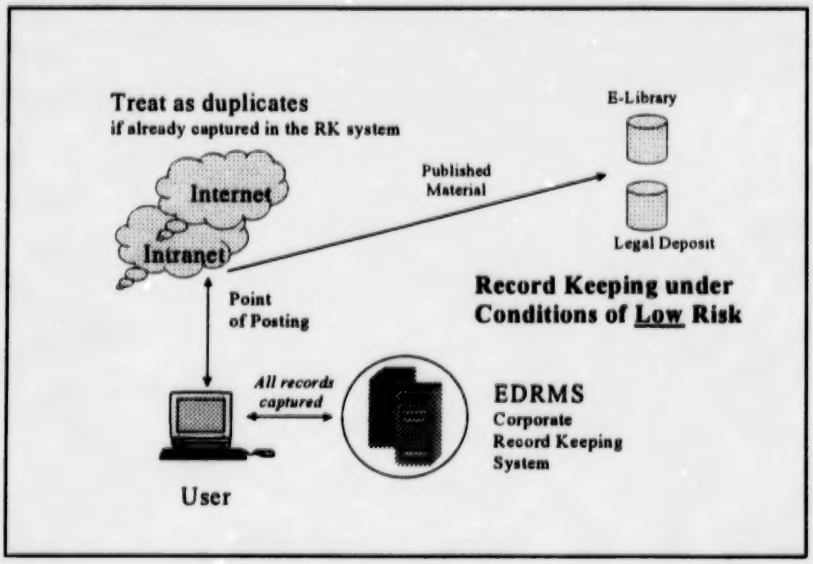
4.2 Document Management

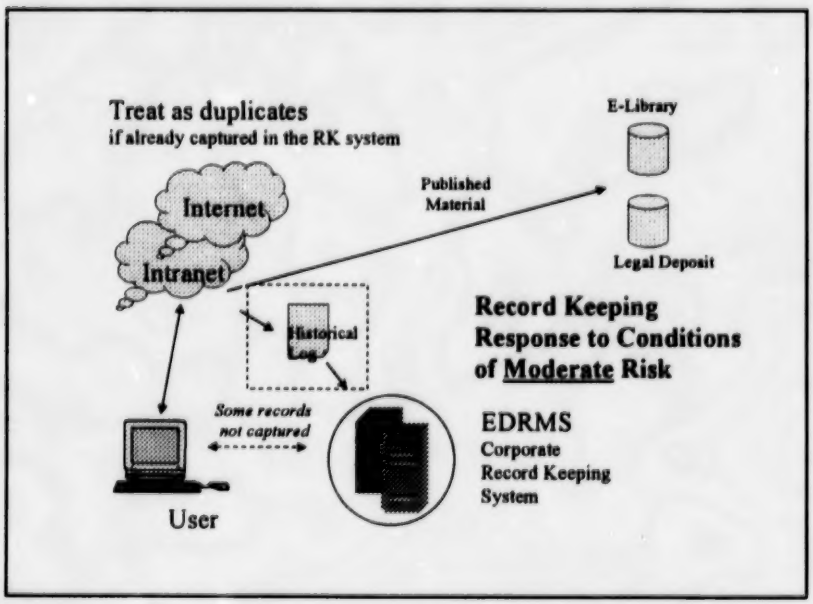
While Web technologies and document management systems have not yet fully merged, it is quite probable that routine desktop authoring through word processing will soon be indistinguishable from more structured approaches, such as HTML, SGML or XML authoring. Rather than publishing on the Internet, organizations will use advanced technology to simply present different views of the same document on a single distributed corporate repository. At that time, publishing strategies will be replaced by viewing strategies, and organizations will need to place greater emphasis on managing the "record."

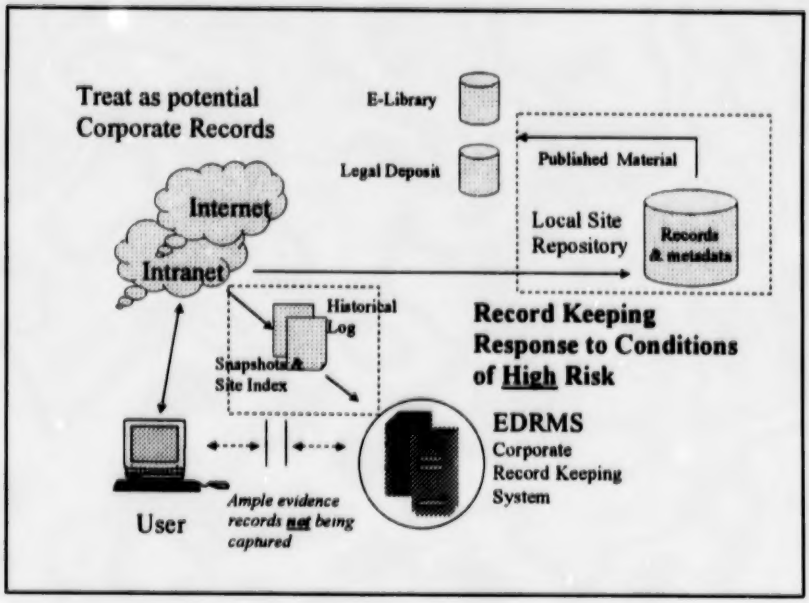
As well, the existing distinctions among electronic document management systems, word processing systems and Web-based distribution systems will likely dissolve rapidly, as applications increasingly reside on the Web. Given the existing pace of convergence, the decision regarding whether to include intranet or Internet documents in the corporate record-keeping system may already be moot. *Unless organizations begin to examine the requirements for organizing information within that environment now, they will soon be playing catch up once again.*

Annex A: Application of the Risk Management Model

The following three diagrams provide a high-level overview of the application of the "Risk Management Model" in support of the IM Forum *Approach to Managing Internet and Intranet Information for Long Term Access and Accountability* and its supporting *Implementation Guide*.






Treat as potential
Corporate Records
E-Library
Legal Deposit
Published Material
Internet
Intranet
Local Site
Repository
Records
& metadata
Historical
Log
Snapshots &
Site Index
Record Keeping
Response to Conditions
of High Risk
EDRMS
Corporate
Record Keeping
System
User
Ample evidence
records not being
captured

Annex B: Web Administrator's Checklist

- **Level of Accountability Exposure and Risk**

  For each Website under their direct control, Web administrators, with the cooperation of content managers and records officers, should:

  a. decide whether the existing level of "accountability exposure" is *low*, *moderate* or *high* (see Figure 1, "Accountability Exposure Analysis, and Record-keeping and Publication Management Response"); and

  b. document their rationale for determining the risk and recommend steps for mitigating risk, such as capturing an historical log, using snapshots or using a local site repository.

1. All Levels of Risk

For all levels of risk, Web administrators should take the following actions:

a. **Establish an accountable content manager for each information item.** The accountable content manager is authorized to create or change the posted document.

b. **Certify the appropriateness of the material.** Confirm with the accountable content manager that the Web submission complies with applicable departmental intranet and Internet publishing guidelines, standards and policies.

   i. **For Internet materials**, certify that the information is appropriate for release to the public.

   ii. **For intranet materials**, certify that the information is appropriate for internal departmental use.

c. **Certify the accuracy and completeness of the material.** Confirm with the accountable content manager that the document and its associated metadata are accurate, current and complete, and that they convey authorized direction.

   i. **Metadata.** Ensure that the content manager has provided sufficient information (metadata) about the item to allow users to easily identify the item's origin, context, content and disposition.

d. **Maintain currency.** Ensure that the accountable content manager has established the following to make it possible to maintain the currency of the posting:

i. **A posting date.** The posting date, or date of publication, should be clearly visible. When appropriate, all major revisions to the material should be identified.

ii. **A review date.** The content manager should commit to reviewing the posted document on the review date for continued relevance, accuracy and timeliness.

iii. **Quality assurance.** The content manager should commit to regularly removing or updating out-of-date information.

e. **Provide for long-term access.** Where long term access should be considered:

i. **Legal Deposit.** Has the content manager or departmental library identified all "publications" that are subject to Legal Deposit, and is there a process for transferring such material?

ii. **E-library.** Has the content manager or departmental library identified all materials that should be copied to the departmental e-library, and is there a process for transferring such material?

2. Low-risk Situations

Where the risk of accountability exposure for an individual site is low, the Web Administrator should take the following actions:

a. **Conduct an annual review.** Annually review the risk level to confirm that it remains low.

b. **Confirm that the content manager has met all departmental corporate record-keeping practices.** These include *certifying* that:

i. the corporate record-keeping system has captured a copy of the posted record and its associated metadata;

ii. a subject classification identifier metadata element has been completed to confirm the record capture; and

iii. the metadata of the source document have been updated to reflect the requested posting activity (note that, on removal, the metadata should be updated again to reflect the change in status).

c. **Dispose of records from the active Website.** Ensure that there are processes for managing the disposition of outdated records from the active Website.

3. Moderate-risk Situations

When the risk of accountability exposure for an individual site is moderate, the Web administrator should take the following actions:

a. **Conduct an annual review.** Annually review the risk level to confirm that it remains moderate and establish processes for reducing risk.

b. **Confirm that the content manager has met all departmental corporate record-keeping practices.** These include *certifying* that:

i. the corporate record-keeping system has captured a copy of the posted record and its associated metadata;

ii. a subject classification identifier metadata element has been completed to confirm the record capture; and

iii. the metadata of the source document have been updated to reflect the requested posting activity (note that, on removal, the metadata should be updated again to reflect the change in status).

c. **Maintain an historical log.** Maintain an historical log for the Website and ensure that the corporate record-keeping system captures it on a regular schedule.

d. **Dispose of records from the active Website.** Ensure that there are processes for managing the disposition of outdated records from the active Website.

e. **Improve integration.** Confirm that the necessary steps have been taken to improve the existing level of integration with the corporate record-keeping system.

4. High-risk Situations

When the risk of accountability exposure for an individual site is high, the Web administrator should consider the following questions:

a. **Is the risk a result of intense public scrutiny?** If so, the Web administrator, in cooperation with records officers and content managers, should schedule the capture of periodic snapshots and site indexes, and transfer both to the corporate record-keeping system.

b. **Is the risk a result of inadequate integration with the corporate record-keeping system?** If so, the Web administrator, in cooperation with records officers and content managers, should implement the following processes:

i. **Use a local site repository.** Until the corporate record-keeping system is fully integrated with the Website, the Web administrator should ensure that a copy of the posted document and its metadata are mirrored to the local site repository when they are posted. (Note that when an organization maintains only those records that have not been captured by the corporate record-keeping system, the Web administrator should segregate records for selective capture and ask the content manager to certify that records have been kept for the remainder.)

ii. **Ensure metadata are complete.** Ensure that the content manager has completed all of the required metadata elements.

iii. **Manage the local site repository.** Ensure that there are processes governing the retention and disposition of Web-based records in the local site repository, in accordance with departmental policies.

iv. **Provide for long-term access.** When there is a requirement to transfer published material from the local site repository to Legal Deposit or to the departmental e-library, make sure processes exist to do so.

v. **Dispose of records from the active Website.** Make sure there are processes for managing the disposition of outdated Web-based records from the active Website.

vi. **Improve integration.** Take the necessary steps to rebuild the existing corporate record-keeping system and develop processes for closer integration with the Web.

vii. **Manage dynamic documents**. Ensure there are processes for assessing the record-keeping requirements of dynamic documents and that the department is using those processes.

Annex C: Glossary

This glossary contains short definitions of key Internet and intranet words, phrases, abbreviations and acronyms. Most of these are not defined elsewhere in this guide.

Accountability
This is a relationship based on the obligation to answer for the exercise of responsibilities conferred.

Source: Government of Canada, *Final Report of the Council of Administrative Renewal*, 1995.

Disposition
In accordance with the *National Archives of Canada Act (1987)*, the National Archives is charged with various responsibilities regarding the disposal of government information, including the authorization of records destruction by government institutions and the preservation of records for their archival or historic importance. (See sections 5 and 6 of the National Archives of Canada Act.) To meet these legislative requirements, the National Archivist issues Records Disposition Authorities to enable government institutions to dispose of records which no longer have operational value, either by permitting their destruction (at the discretion of institutions), by requiring their transfer to the National Archives, or by agreeing to their alienation from the control of the Government of Canada.

Source: *The Government Records Disposition Program of the National Archives of Canada*, approved by the Acting National Archivist, May 14, 1999.

Document
(1) A combination of a medium and the information recorded on or in it, which may be used as evidence or for consultation.

(2) A single archival record or manuscript item, which is usually physically indivisible.

Source: International Council on Archives, *Dictionary of Archival Terminology*, 1988.

Note that document management systems treat various files and data associated with one document as a single object during archival and retrieval transactions. Such functionality is required because complex electronic documents often consist of several files—such as chapters, diagrams and photographs—stored in different file formats. To manage such documents efficiently, a document management system must keep track of each file, presenting the document to users as though it were a single entity.

Source: National Library of Canada, *Document Management Systems*, <http://www.nlc-bnc.ca/pubs/netnotes/notes44.htm>.

E-library
An e-library encompasses the functions of selection, bibliographic control, electronic storage, access, service and preservation. Publications stored on the e-library's server can be linked to records in a public access catalogue (online or Web based) and made available to users. The server may be an Internet server managed by the departmental library, part of a departmental Internet server or part of an integrated library system.

Extranet
An extranet is an intranet that is partially accessible to authorized outsiders. Whereas an intranet resides behind a firewall and is accessible only to members of the same company or organization, an extranet provides various levels of accessibility to outsiders. You can access an extranet using a valid user name and password; your identity determines which parts of the extranet you can view.

Source: The Internet.com PC Web/opaedia at <http://www.pcwebopaedia.com/>.

Government Record *(see also Record)*
Within the context of the definition of "record" in the *National Archives of Canada Act* and the *Access to Information Act*, a "government record" is recorded information, regardless of physical form, that is under the control of a government institution, and is collected, created, received and/or used in the initiation, conduct or completion of an institutional activity. In order to meet business and accountability requirements, government records must have sufficient content, context, and structure to provide evidence of the activity.

Source: Government of Canada, National Archives of Canada, Information Management Standards and Practices Division, *Record Keeping in the Electronic Work Environment—Vision*, 1996.

Internet
This is a global collection of computer networks that exchange information using the TCP/IP suite of networking protocols.

Source: NETGLOS Multilingual Glossary of Internet Terminology at <http://wwli.com/translation/netglos/glossary/glossary.html#I>.

Intranet
This is a network based on TCP/IP protocols that belongs to an organization, usually a corporation, and that is accessible only to the organization's members, employees or other authorized users. An intranet's Websites look and act just like any other Website, but the firewall surrounding an intranet fends off unauthorized access.

Source: The Internet.com PC Web/opaedia at <http://www.pcwebopaedia.com/>.

Local Site Repository
This is an electronic repository established under the control of an individual government department to temporarily manage copies of that department's electronically recorded information as corporate records until the corporate record-keeping system is adequate for the task. It is intended to replicate, at time of posting, all material posted to an active

Website. Contained in a separate storage device, a local site repository:

- provides a means of reconstructing the information content of an active Website; and
- helps a department dispose of recorded information through:
  - controlled deletion,
  - transfer of archival records to the National Archives (in the case of record material),
  - the identification of publications for Legal Deposit (in the case of published material), and
  - the identification and replication of material of ongoing informational value required to support a departmental e-library.

Posting
Posting refers to making recorded information available on an Internet, intranet or extranet, whether or not access is provided through direct access to the source document or to a certified copy of the document.

Publication (and related concepts)
"Published in Canada" means "released in Canada for public distribution or sale, otherwise than by her Majesty in right of a province or municipality."
Source: *National Library of Canada Act* (1994).

A networked electronic publication is a digitally encoded information resource made available to the public through a communication network.
Source: National Library of Canada, Electronic Collections Coordinating Group, Networked Electronic Publications Policy and Guidelines, October 1998.

Published material refers to an information product that has been created and edited for the purpose of distribution or sale. Material published by or for federal institutions is deposited in federal library collections.
Source: Treasury Board of Canada, Secretariat, Policy on the Management of Government Information Holdings, 1994.

Information products are documents that have been compiled from available information or data sources and that are being published for a defined audience and a stated purpose.
Source: Health Canada, Records Management Policy, September 1998.

Record *(see also Government Record, Source Record, Record Keeping)*
A record includes any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microform, sound recording, videotape, machine-readable record and any other documentary material, regardless of physical form or characteristics, and any copy thereof.

Source: *National Archives of Canada Act (1987)*.

Source Record
In relation to a record, this is the record itself or any facsimile intended by the author of the record to have the same effect. In relation to a record produced by a computer system, this is any printout or any other intelligible output that accurately reproduces, whether in the same or a modified form, the data supplied to the computer system.

Source: Canadian Institute of Chartered Accountants, *Audit Implications of Electronic Document Management*, 1997.

Record Keeping
Record keeping is the act of documenting an activity by creating, collecting or receiving records and ensuring that they are available, understandable and usable for as long as they are needed.

Source: Government of Canada, *Final Report of the AGBR Terminology Working Group*, April 9, 1996.

Retention Period
This is the length of time, determined by an institution, that the institution needs to retain a record for operational or legal reasons.

Specifically, the determination of retention periods occurs within the context of an institution's business risk analysis and assessment of its information resource requirements, taking into account federal information law as well as other statutes or regulations which may have application to the retention of records. RDAs issued by the National Archivist to government institutions do not provide an approval for the retention periods which are necessary to the life-cycle management and disposal of records by institutions.

Source: *The Government Records Disposition Program of the National Archives of Canada*, approved by the Acting National Archivist, May 14, 1999.

Annex D: References and Authorities

This section lists authoritative sources and references used to develop *An Approach to Managing Internet and Intranet Information for Long-term Access and Accountability* and its supporting *Implementation Guide*.

Legislative Acts

National Archives of Canada Act (1987)
National Library of Canada Act
Access to Information Act
Official Languages Act
Privacy Act
Copyright Act

Other References and Authorities

Canadian Institute of Chartered Accountants, *Audit Implications of Electronic Document Management* (including an extract from the *Proposed Uniform Electronic Evidence Act*), 1997.

Duranti, L. (University of British Columbia). Extracted from National Archives of Canada, *Approach to the Description and Classification of Government Records*, February 1999.

Health Canada, Records Management Policy, September 1998.

McClure, Charles R. and J. Timothy Sprehe, *Analysis and Development of Model Quality Guidelines for Electronic Records Management on State and Federal Websites*, January 1998, <http://istweb.syr.edu/~mcclure/nhprc/nhprc_chpt_6.html>.

National Archives of Canada, *Alternate Service Delivery—Record Keeping Issues and Questions, A Summary Checklist*, August 20, 1998.

National Archives of Canada, *Approach to the Description and Classification of Government Records*, February 1999.

National Archives of Canada, *Authority for the Destruction of Transitory Records*, December 1990.

National Archives of Canada, *Functional Requirements for Record Keeping in the Government of Canada*, undated.

National Archives of Canada, Information Management Standards and Practices Division, Records/Documents/Information Management (RDIM): Integrated Document Management System for the Government of Canada—Request for Proposal (RFP), Software Requirements, May 1996.

National Archives of Canada, *Networked Electronic Information, Perspective of the National Archives and the National Library (Draft)*, December 1997.

National Library of Canada, Electronic Collections Coordinating Group, Networked Electronic Publications Policy and Guidelines, October 1998.

Treasury Board of Canada, Secretariat, *Blueprint for Renewing Government Services Using Technology (Discussion Draft)*, undated.

Treasury Board of Canada, Secretariat, *Government of Canada Internet Guide*, <http://canada.gc.ca/program/guide>.

Treasury Board of Canada, Secretariat, *Information Policy Framework*, June 4, 1996.

Treasury Board of Canada, Secretariat, Policy on the Management of Government Information Holdings, 1994.

Treasury Board of Canada, Secretariat, Policy on the Use of Electronic Networks, 1998, <http://www.tbs-sct.gc.ca/Pubs_pol/ciopubs/TB_CP/UENE.html>.

C:\WINDOWS\Temporary Internet Files\Content.IE5\F79OBK8P\implement2_e[1].wpd